Distribution of Primes in Certain Number Classes.

by

Georgia A. Caldwell

A.B., University of Kansas,

June, 1928.

Submitted to the Department of Mathematics and the Faculty of the Graduate School of the University of Kansas in partial fulfillment of the requirements for the degree of Master of Arts.

Approved by:

W. H. Mitchell
Instructor in charge.

C. H. Ashton
Chairman of Dept.

June 3, 1929.

Table of Contents

Distribution of Primes in Certain Number Classes.

The interest of mathematicians in the study of the frequency and determination of prime numbers may be explained by the seeming simplicity of a problem which has not been solved by the efforts of the most profound thinkers. For centuries mathematicians have worked with the problems involved in the study of prime numbers and through their efforts, many interesting discoveries have been added to the field of Number Theory. However, the problem is not solved in its entirety.

Eratosthenes,[1] about 200 B. C., was the first to contribute a usable method for the determination of prime numbers. His method is known as the "sieve of Eratosthenes". He took a list of consecutive natural numbers and crossed out every second number after two, thereby eliminating the multiples of two. He then crossed out every third number after three, every fifth number after five, etc. Since the largest prime a number can contain is the largest prime less than its square root, this method determined the primes up to the square of the first prime after the last one whose multiples were crossed out.

Fermat[2] in 1640 offered the formula $2^{2^n} + 1$, which he believed always expressed prime numbers, although he admitted he had no proof for it.

---

1. Gow, A Short History of Greek Mathematics (1923) page 87.
2. Oeuvres de Fermat (1894), Fermat a' Frenicle page 206.

Euler[3] disproved this by factoring the fifth Fermat number. Since,[4] twelve Fermat numbers have been proved composite, while none but the first four have been proved prime.

Euler[5] suggested $2x^2 + 29$, $x^2 + x + 41$, $x^2 + x + 17$, as formulae for prime numbers.

Lucas[6] proved that an algebraic expression cannot always represent a prime number.

However, some algebraic expressions do give primes for numerous values of the variable. $x^2 + x + 41$ gives prime numbers for the forty-one values of x, x = 0, 1, 2, ----- 40. $2x^2 + 29$ gives primes for x = 0, 1, ---- 28.

Much work has also been done on the frequency of primes. Lucas[6a] and Legendre[7] prove that the number of primes is infinite. They attribute the proof to Euclid. Let p be any prime whatsoever. Add one to the product of p and all the primes less than p. This number, N, is greater than p, and is either prime or composite. If it is prime, there is a prime greater than p, which is any prime whatsoever, and the theorem is proved. If N is not prime, it is divisible by a prime number. But evidently N is not divisible by p or any of the primes less than p for N divided by any one of these leaves a remainder of one. N must, then, be divisible by a prime greater than p.

---

3. Dickson, Hist. of the Theory of Nos. Vol. I. p. 375. Quotes Opera postuma 1862, p. 169-71.
4. Archibald, Am. Math. Monthly, 21, 1914. p. 247-251.
5. Legendre, Theorie des Nombres (1808) p. 11 Quotes Memoires de Berlin, 1772. p. 36.
6. Lucas, Theorie des Nombres (1891) p. 355.
6a. Ibid.
7. Legendre, Theorie des Nombres (1808) p. 11 and 12.

Perrot[8] proved the number of primes infinite by a method somewhat different from Euclid's. He proved that there are at least n - 1 primes between q_n and M where $M = q_1 \cdot q_2 \cdots q_n$ and the q's are prime numbers.

Lucas[9] proved that there is an infinite number of primes of the form 5h + 2, and also of the form 8h + 7.

Sylvester[10] proved that if an arithmetical progression contains more than one prime, it contains an infinite number.

G. Metrod[11] offered two further proofs of the fact that the number of primes is infinite.

A method suggested by Legendre[12] for finding the number of primes less than a given number is the following. Let the given number be N. Then there are N/2 numbers divisible by two. There are N/3 numbers divisible by three but half of these have already been removed as multiples of two. We must then add back N/2.3 numbers. Likewise, there are N/5 numbers divisible by five but as we have already removed those divisible by two and three, we must add back the numbers divisible by ten and fifteen. Then the multiples of thirty have been subtracted and added back. It is therefore necessary to subtract them again. By continuing this

8. American Journal of Math. 13, (1891) p. 303-305.
9. Ibid. 1, (1878) p. 309.
10. Messenger of Mathematics(2) 1, (1872) p. 143-144.
11. L' intermediaire des Math. 24, (1917) p. 39-40.
12. Legendre, Theorie des Nombres, (1808) p. 6 - 8.

process, Legendre developed the formula:

$$N - \Sigma\left[\frac{N}{p}\right] + \Sigma\left[\frac{N}{pq}\right] - \Sigma\left[\frac{N}{pqr}\right] + \cdots .$$

To this the number of primes used is added for these primes have been subtracted.

13. Sylvester obtained the following formula for the number of primes between n and 2n:

$$n - \Sigma H\frac{n}{a} + \Sigma H\frac{n}{ab} - \Sigma H\frac{n}{abc} + \cdots,$$

where a, b, c, ---- p are all the primes from 2 to p, and p^2 is not greater than 2n.

14. Tchebycheff gave the formula:

$$x\left[\frac{1}{\log x} + \frac{1}{\log^2 x} + \frac{1\cdot 2}{\log^3 x} + \frac{1\cdot 2\cdot 3}{\log^4 x} + \cdots\right].$$

Work has also been done on the verification of large primes.

15. G. Rados stated that p is prime if and only if

$$\{1!\ 3!\ 4!\ \cdots\cdots\ (p-2)!\,(p-1)!\}^4 \equiv 1 \pmod{p}.$$

16. Lucas proved theorems concerning the factoribility of numbers of certain forms and 17. Carmichael proved similar theorems.

---

13. Lucas, Theorie des Nombres p. 411-12.
14. Tchebycheff in Liouville Journal le Math. XVII (1852) 358-361.
15. Dickson, Hist. of the Theory of Nos. Quotes Math.'es Termes Ertesitö 34, 1916, 62-70.
16. Am. Journal of Math. (1878) 184-240, 289-321.
17. Annals of Math. (2), 15. pages 62-63.

Dr. U. G. Mitchell has suggested to me the problem of investigating whether or not the number of primes in certain kinds of number intervals depends on the number of primes in the intervals preceding, and whether the number of primes in the interval can be found by a knowledge of the primes in preceding intervals.

It is the purpose of this study to examine the number of primes in three types of intervals, the powers of two, the factorials, and the powers of five, by a method analogous to the "sieve of Eratosthenes". In each case, the numbers of two factors were eliminated, the numbers of three factors, etc., until only the primes were left. Here, however, the object is to find the number of primes rather than what they are. A knowledge of the primes in preceding cells is assumed.

A study was also made of Fermat numbers in an attempt to find out what numbers of the form $2^n \cdot p + 1$ could be factors of Fermat numbers.

II. Number of Primes Less Than 2^n.

1. The number of primes less than a given number, 2^n, was found by eliminating the composites of two factors, the composites of three factors, and so on to the composites of n - 1 factors. The first number of n factors is, of course, 2^n. Consequently, no number less than 2^n can have more than n - 1 factors. The number of composites less than 2^n was subtracted from $2^n - 1$ to determine the number of primes less than 2^n.

Composites less than 2^n would be of the form $(2 + a_1)(2 + a_2)$, $(2 + a_1)(2 + a_2)(2 + a_3)$, $(2 + a_1)(2 + a_2)\cdots(2 + a_{n-1})$. The values which a_k, $k = 1, 2, \text{---} n - 1$, might take on were found in each case.

2. Following are several examples to illustrate the method used in compiling table I, which gives the number of composites less than each number 2^n, $n \leq 12$.

$n_2 = 2^2 = 4$

Four is the smallest number of two factors. Consequently, all numbers less than four are prime.

$n_3 = 2^3 = 8$

Composites of two factors:	No. of combinations
$a_1 = 0$, $a_2 = 0$, 1	2
$a_1 = 1$, $a_2 = 0$.	

$n_4 = 2^4 = 16$

Composites of two factors:	No. of combinations
$a_1 = 0,\ a_2 = 0, 1, 3, 5.$	6
$a_1 = 1,\ a_2 = 0, 1, 3.$	
$a_1 = 3,\ a_2 = 0, 1.$	
$a_1 = 5,\ a_2 = 0.$	
Composites of three factors:	
$a_1 = 0,\ a_2 = 0,\ a_3 = 0, 1.$	2
$a_1 = 0,\ a_2 = 1,\ a_3 = 0.$	

$n_5 = 2^5 = 32$

Composites of two factors:	
$a_1 = 0,\ a_2 = 0, 1, 3, 5, 9, 11.$	10
$a_1 = 1,\ a_2 = 0, 1, 3, 5.$	
$a_1 = 3,\ a_2 = 0, 1, 3.$	
$a_1 = 5,\ a_2 = 0, 1.$	
$a_1 = 9,\ a_2 = 0.$	
$a_1 = 11,\ a_2 = 0.$	
Composites of three factors:	
$a_1 = 0,\ a_2 = 0,\ a_3 = 0, 1, 3, 5.$	7
$a_1 = 0,\ a_2 = 1,\ a_3 = 0, 1, 3.$	
$a_1 = 0,\ a_2 = 3,\ a_3 = 0, 1.$	
$a_1 = 1,\ a_2 = 1,\ a_3 = 0, 1.$	
$a_1 = 1,\ a_2 = 3,\ a_3 = 0.$	

Composites of four factors: No. of combinations

$a_1 = 0,\ a_2 = 0,\ a_3 = 0,\ a_4 = 0, 1.$ 2

$a_1 = 0,\ a_2 = 0,\ a_3 = 1,\ a_4 = 0.$

$n_{12} = 2^{12} = 4096$

Composites of two factors:

$a_1 = 0,\ a_2 = 0 - 2037$

This is to mean that a_2 takes all values from 0 to 2037 such that $a_2 + 2$ is prime.

$a_1 = 1,\ a_2 = 1 - 1359;$ $a_1 = 3,\ a_2 = 3 - 819;$ 1124

$a_1 = 5,\ a_2 = 5 - 575;$ $a_1 = 9,\ a_2 = 9 - 365;$

$a_1 = 11,\ a_2 = 11 - 311;$ $a_1 = 15,\ a_2 = 15 - 237;$

$a_1 = 17,\ a_2 = 17 - 209;$ $a_1 = 21,\ a_2 = 21 - 171;$

$a_1 = 27,\ a_2 = 27 - 137;$ $a_1 = 29,\ a_2 = 29 - 129;$

$a_1 = 35,\ a_2 = 35 - 107;$ $a_1 = 39,\ a_2 = 39 - 95;$

$a_1 = 41,\ a_2 = 41 - 87;$ $a_1 = 45,\ a_2 = 45 - 81;$

$a_1 = 51,\ a_2 = 51 - 71;$ $a_1 = 57,\ a_2 = 57 - 65;$

$a_1 = 59,\ a_2 = 59 - 65.$

Composites of three factors:

$a_1 = 0,\ a_2 = 0,\ a_3 = 0 - 1019;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 1 - 675;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 3 - 407;$

$a_1 = 0,\ a_2 = 5,\ a_3 = 5 - 281;$

$a_1 = 0,\ a_2 = 9,\ a_3 = 9 - 179;$

$a_1 = 0,\ a_2 = 11,\ a_3 = 11 - 155;$

$a_1 = 0,\ a_2 = 15,\ a_3 = 15 - 111;$

Composite of three factors (cont'd)	No. of combinations
$a_1 = 0, a_2 = 17, a_3 = 17 - 105;$	1049
$a_1 = 0, a_2 = 21, a_3 = 21 - 87;$	
$a_1 = 0, a_2 = 27, a_3 = 27 - 65;$	
$a_1 = 0, a_2 = 29, a_3 = 29 - 59;$	
$a_1 = 0, a_2 = 35, a_3 = 35 - 51;$	
$a_1 = 0, a_2 = 39, a_3 = 39 - 45;$	
$a_1 = 0, a_2 = 41, a_3 = 41 - 45;$	
$a_1 = 1, a_2 = 1, a_3 = 1 - 447;$	
$a_1 = 1, a_2 = 3, a_3 = 3 - 269;$	
$a_1 = 1, a_2 = 5, a_3 = 5 - 191;$	
$a_1 = 1, a_2 = 9, a_3 = 9 - 111;$	
$a_1 = 1, a_2 = 11, a_3 = 11 - 101;$	
$a_1 = 1, a_2 = 15, a_3 = 15 - 77;$	
$a_1 = 1, a_2 = 17, a_3 = 17 - 69;$	
$a_1 = 1, a_2 = 21, a_3 = 21 - 57;$	
$a_1 = 1, a_2 = 27, a_3 = 27 - 45;$	
$a_1 = 1, a_2 = 29, a_3 = 29 - 41;$	
$a_1 = 3, a_2 = 3, a_3 = 3 - 161;$	
$a_1 = 3, a_2 = 5, a_3 = 5 - 111;$	
$a_1 = 3, a_2 = 9, a_3 = 9 - 71;$	
$a_1 = 3, a_2 = 11, a_3 = 11 - 59;$	
$a_1 = 3, a_2 = 15, a_3 = 15 - 45;$	
$a_1 = 3, a_2 = 17, a_3 = 17 - 41;$	
$a_1 = 3, a_2 = 21, a_3 = 21 - 29;$	

Composite of three factors (cont'd) No. of combinations

$a_1 = 5, a_2 = 5, a_3 = 5 - 81;$

$a_1 = 5, a_2 = 9, a_3 = 9 - 51;$

$a_1 = 5, a_2 = 11, a_3 = 11 - 41;$

$a_1 = 5, a_2 = 15, a_3 = 15 - 29;$

$a_1 = 5, a_2 = 17, a_3 = 17 - 27;$

$a_1 = 5, a_2 = 21, a_3 = 21;$

$a_1 = 9, a_2 = 9, a_3 = 9 - 29;$

$a_1 = 9, a_2 = 11, a_3 = 11 - 21;$

$a_1 = 9, a_2 = 15, a_3 = 15 - 17;$

$a_1 = 9, a_2 = 17, a_3 = 17;$

$a_1 = 11, a_2 = 11, a_3 = 11 - 21;$

$a_1 = 11, a_2 = 15, a_3 = 15.$

Composites of four factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0 - 507;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1 - 335;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 3 - 197;$

$a_1 = 0, a_2 = 0, a_3 = 5, a_4 = 5 - 137;$

$a_1 = 0, a_2 = 0, a_3 = 9, a_4 = 9 - 87;$

$a_1 = 0, a_2 = 0, a_3 = 11, a_4 = 11 - 71;$

$a_1 = 0, a_2 = 0, a_3 = 15, a_4 = 15 - 57;$

$a_1 = 0, a_2 = 0, a_3 = 17, a_4 = 17 - 51;$

$a_1 = 0, a_2 = 0, a_3 = 21, a_4 = 21 - 41;$

$a_1 = 0, a_2 = 0, a_3 = 27, a_4 = 27 - 29;$

Composits of four factors (cont'd) No. of combinations.

$a_1 = 0,\ a_2 = 1,\ a_3 = 1,\ a_4 = 1 - 225;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 3,\ a_4 = 3 - 129;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 5,\ a_4 = 5 - 95;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 9,\ a_4 = 9 - 59;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 11,\ a_4 = 11 - 45;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 15,\ a_4 = 15 - 35;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 17,\ a_4 = 17 - 29;$

$a_1 = 0,\ a_2 = 1,\ a_3 = 21,\ a_4 = 21 - 27;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 3,\ a_4 = 3 - 77;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 5,\ a_4 = 5 - 51;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 9,\ a_4 = 9 - 35;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 11,\ a_4 = 11 - 29;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 15,\ a_4 = 15 - 21;$

$a_1 = 0,\ a_2 = 3,\ a_3 = 17,\ a_4 = 17;$

$a_1 = 0,\ a_2 = 5,\ a_3 = 5,\ a_4 = 5 - 39;$

$a_1 = 0,\ a_2 = 5,\ a_3 = 9,\ a_4 = 9 - 21;$

$a_1 = 0,\ a_2 = 5,\ a_3 = 11,\ a_4 = 11 - 17;$

$a_1 = 0,\ a_2 = 5,\ a_3 = 15,\ a_4 = 15;$

$a_1 = 0,\ a_2 = 9,\ a_3 = 9,\ a_4 = 9 - 11;$

$a_1 = 0,\ a_2 = 9,\ a_3 = 11,\ a_4 = 11;$

$a_1 = 1,\ a_2 = 1,\ a_3 = 1,\ a_4 = 1 - 149;$

$a_1 = 1,\ a_2 = 1,\ a_3 = 3,\ a_4 = 3 - 87;$

$a_1 = 1,\ a_2 = 1,\ a_3 = 5,\ a_4 = 5 - 59;$

Composite of four factors (cont'd) No. of combinations.

$a_1 = 1, a_2 = 1, a_3 = 9, a_4 = 9\text{-}39;$ 669

$a_1 = 1, a_2 = 1, a_3 = 11, a_4 = 11 - 29;$

$a_1 = 1, a_2 = 1, a_3 = 15, a_4 = 15 - 21;$

$a_1 = 1, a_2 = 1, a_3 = 17, a_4 = 17 - 21;$

$a_1 = 1, a_2 = 3, a_3 = 3, a_4 = 3 - 51;$

$a_1 = 1, a_2 = 3, a_3 = 5, a_4 = 5 - 35;$

$a_1 = 1, a_2 = 3, a_3 = 11, a_4 = 11 - 17;$

$a_1 = 1, a_2 = 5, a_3 = 5, a_4 = 5 - 21;$

$a_1 = 1, a_2 = 5, a_3 = 9, a_4 = 9 - 15;$

$a_1 = 1, a_2 = 5, a_3 = 11, a_4 = 11;$

$a_1 = 1, a_2 = 9, a_3 = 9, a_4 = 9;$

$a_1 = 3, a_2 = 3, a_3 = 3, a_4 = 3 - 29;$

$a_1 = 3, a_2 = 3, a_3 = 5, a_4 = 5 - 21;$

$a_1 = 3, a_2 = 3, a_3 = 9, a4 = 9 - 11;$

$a_1 = 3, a_2 = 5, a_3 = 5, a_4 = 5 - 11;$

$a_1 = 5, a_2 = 5, a_3 = 5, a_4 = 5 - 9;$

Composites of five factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = o, a_5 = 0 - 249;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1 - 165;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 3, a_5 = 3 - 99;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 3, a_5 = 5 - 71;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 9, a_5 = 9 - 41;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 11, a_5 = 11 - 35;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 15, a_5 = 15 - 27;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 17, a_5 = 17 - 21;$

Composites of five factors: No. of combinations

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1 - 111;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 3, a_5 = 3 - 65;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 5, a_5 = 5 - 45;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 9, a_5 = 9 - 29;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 11, a_5 = 11 - 21;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 15, a_5 = 15 - 17;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 3, a_5 = 3 - 35;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 5, a_5 = 5 - 27;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 9, a_5 = 9 - 15;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 11, a_5 = 11;$

$a_1 = 0, a_2 = 0, a_3 = 5, a_4 = 5, a_5 = 5 - 17;$

$a_1 = 0, a_2 = 0, a_3 = 5, a_4 = 9, a_5 = 9 - 11;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1 - 71;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 3, a_5 = 3 - 41;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 5, a_5 = 5 - 29;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 9, a_5 = 9 - 17;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 11, a_5 = 11 - 15;$

$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 3, a_5 = 3 - 21;$

$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 5, a_5 = 5 - 17;$

$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 0, a_5 = 9;$

$a_1 = 0, a_2 = 1, a_3 = 5, a_4 = 5, a_5 = 5 - 11;$

$a_1 = 0, a_2 = 3, a_3 = 3, a_4 = 3, a_5 = 3 - 11;$

$a_1 = 0, a_2 = 3, a_3 = 3, a_4 = 5, a_5 = 5 - 9;$

$a_1 = 0, a_2 = 3, a_3 = 5, a_4 = 5, a_5 = 5;$

Composites of five factors: No. of combinations

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1 - 45;$ 367

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 3, a_5 = 3 - 27;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 5, a_5 = 5 - 17;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 9, a_5 = 9 - 11;$

$a_1 = 1, a_2 = 1, a_3 = 3, a_4 = 3, a_5 = 3 - 15;$

$a_1 = 1, a_2 = 1, a_3 = 3, a_4 = 5, a_5 = 5 - 11;$

$a_1 = 1, a_2 = 1, a_3 = 5, a_4 = 5, a_5 = 5;$

$a_1 = 1, a_2 = 3, a_3 = 3, a_4 = 3, a_5 = 3 - 5;$

$a_1 = 1, a_2 = 3, a_3 = 3, a_4 = 5, a_5 = 5;$

$a_1 = 3, a_2 = 3, a_3 = 3, a_4 = 3, a_5 = 3;$

Composites of six factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0 - 125;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 1 - 81;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 3, a_6 = 3 - 45;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 5, a_6 = 5 - 29;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 9, a_6 = 9 - 21;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 11, a_6 = 11 - 17;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 1 - 51;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 3, a_6 = 3 - 29;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 5, a_6 = 5 - 21;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 9, a_6 = 9 - 11;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 11, a_6 = 11;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 3, a_5 = 3, a_6 = 3 - 17;$

Composites of six factors (cont'd) No. of combinations.

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 3, a_5 = 5, a_6 = 5 - 11;$ 177

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 5, a_5 = 5, a_6 = 5;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1 - 35;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 3, a_6 = 3 - 17;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 5, a_6 = 5 - 11;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 3, a_5 = 3, a_6 = 3 - 11;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 3, a_5 = 5, a_6 = 5;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 3, a_5 = 3, a_6 = 3 - 5;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1 - 21;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 3, a_6 = 3 - 11;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 5, a_6 = 5;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 3, a_5 = 3, a_6 = 3 - 5;$

$a_1 = 0, a_2 = 1, a_3 = 3, a_4 = 3, a_5 = 3, a_6 = 3;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1 - 11;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 3, a_6 = 3 - 5;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 5, a_6 = 5;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 3, a_5 = 3, a_6 = 3;$

Composites of seven factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0 - 59;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 1, a_7 = 1 - 39;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 3, a_7 = 3 - 21;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 5, a_7 = 5 - 15;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 9, a_7 = 9;$

Composites of seven factors: No. of combinations

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 1, a_7 = 1 - 21$ 83

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 3, a_7 = 3 - 15;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 5, a_7 = 5 - 9;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 3, a_6 = 3, a_7 = 3 - 5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 3, a_6 = 5, a_7 = 5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1 - 15;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 3, a_7 = 3 - 9;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 5, a_7 = 5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 3, a_6 = 3, a_7 = 3;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1 - 9;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 3, a_7 = 3 - 5;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1 - 5;$

$a_1 = 0, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 3, a_7 = 3;$

$a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1 - 3;$

Composites of eight factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0, a_8 = 0-29;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 1, a_8 = 1 - 17;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 3, a_8 = 3 - 9;$

$a_1 = 0, a_2 = 0, a_3 = 3, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 5, a_8 = 5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 1, a_7 = 1, a_8 = 1 - 11;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 1, a_7 = 3, a_8 = 3 -5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 3, a_7 = 3, a_8 = 3;$ 37

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 1, a_7 = 1, a_8 = 1 - 5;$

Composites of eight factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 1, a_7 = 3, a_8 = 3;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1, a_8 = 1 - 3;$

$a_1 = 0, a_2 = 0, a_3 = 1, a_4 = 1, a_5 = 1, a_6 = 1, a_7 = 1, a_8 = 1.$

Composites of nine factors:

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0, a_8 = 0, a_9 = 0\text{-}11;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0, a_8 = 0, a_9 = 1\text{-}5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 0, a_8 = 3, a_9 = 3;$ 15

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 0, a_7 = 1, a_8 = 1, a_9 = 1\text{-}5;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 0, a_6 = 1, a_7 = 1, a_8 = 1, a_9 = 1;$

$a_1 = 0, a_2 = 0, a_3 = 0, a_4 = 0, a_5 = 1, a_6 = 1, a_7 = 1, a_8 = 1, a_9 = 1;$

Composites of ten factors:

7

$a_1=0, a_2=0, a_3=0, a_4=0, a_5=0, a_6=0, a_7=0, a_8=0, a_9= 0, a_{10}=0\text{-}5;$

$a_1=0, a_2=0, a_3=0, a_4=0, a_5=0, a_6=0, a_7=0, a_8=0, a_9=1, a_{10}= 1\text{-}3;$

$a_1=0, a_2=0, a_3=0, a_4=0, a_5=0, a_5=0, a_7=0, a_8=1, a_9=1, a_{10}= 1;$

Composites of eleven factors:

$a_1=0, a_2=0, a_3=0, a_4=0, a_5=0, a_6=0, a_7= 0, a_8=0, a_9=0, a_{10}=0, a_{11}=0\text{-}1.$ 2

TABLE I.

	Numbers less than										
	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
Primes	3	5	7	12	19	32	55	98	173	310	565
Composites of 2 factors	0	2	6	10	22	42	82	157	304	589	1124
Composites of 3 factors	0	0	2	7	13	30	60	125	256	514	1049
Composites of 4 factors	0	0	0	2	7	14	34	71	152	325	669
Composites of 5 factors	0	0	0	0	2	7	15	36	77	168	367
Composites of 6 factors	0	0	0	0	0	2	7	15	37	80	177
Composites of 7 factors	0	0	0	0	0	0	2	7	15	37	83
Composites of 8 factors	0	0	0	0	0	0	0	2	7	15	37
Composites of 9 factors	0	0	0	0	0	0	0	0	2	7	15
Composites of 10 factors	0	0	0	0	0	0	0	0	0	2	7
Composites of 11 factors	0	0	0	0	0	0	0	0	0	0	2

3. Theorem I.

The number of composites less than 2^n of n-n' factors becomes constant when $n \geqq k$ where k is the first number such that $3^k > 2^{n'+k}$.

Proof:

The number of composites of $n - n'$ factors less than a given number 2^n is found by taking $2^n = 2^{n-(n'+c)} \cdot 2^{n'+c}$ for all values of c from 1 to $n - n'$. If $2^{n-(n'+c)}$ is multiplied by all numbers of c factors less than $2^{n'+c}$, it is evident that we have composites of $n - n'$ factors less than 2^n. However, in counting the numbers of c factors less than $2^{n'+c}$, we omit all those which contain 2 as a factor, except when c is one, for these will have been counted previously with higher powers of two. Since we omit the composites with two as a factor, 3^c is the smallest number of c factors. If $3^c > 2^{n'+c}$, there are no numbers of c factors less than $2^{n'+c}$. Let k be the first value of c such that $3^c > 2^{n'+c}$. We then have $2^n = 2^{n-(n'+k)} \cdot 2^{n'+k}$. To get composites of $n - n'$ factors, we multiply $2^{n-(n'+k)}$ by all numbers of k factors less than $2^{n'+k}$. But there are no such numbers. Also, if $3^k > 2^{n'+k}$, then $3^{k+1} > 2^{n'+k+1}$, $3^{k+2} > 2^{n'+k+2}$, etc. That is, when $c \geqq k$, there are no more composites of $n - n'$ factors less than 2^n. Evidently, k does not depend on n, but on n'. Therefore, if

n is large enough to allow these k divisions of 2^n, i.e., if $n \geq k$, the number of composites of $n - n'$ factors is constant.

Illustration:

The number of composites less than 2^n of n - 3 factors has not become constant when n = 6 but has when n = 10. Let us show that the theorem holds in each of these cases.

A. To find the number of composites of 6 - 3 factors $< 2^6$:

$$2^6 = 2^{6-(3+1)} \cdot 2^{3+1}.$$

Multiply 2^2 by all primes $< 2^4$ to get composites of three factors $< 2^6$.

$$2^6 = 2^{6-(3+2)} \cdot 2^{3+2}.$$

Multiply 2 by all numbers of two factors $< 2^5$, omitting multiples of two as they were considered when $2^{6-(3+1)}$ was multiplied by primes.

$$2^6 = 2^{6-(3+3)} \cdot 2^{3+3}.$$

This is the last division of 2^6 but $3^3 \not> 2^{3+3}$ so the number of composites of three factors less than 2^6 is not constant.

B. To find the number of composites of 10 - 3 factors $< 2^{10}$:

$$2^{10} = 2^{10-(3+1)} \cdot 2^{3+1}.$$

Multiply $2^{10-(3+1)}$ by all primes less than 2^4.

$$2^{10} = 2^{10-(3+2)} \cdot 2^{3+2}.$$

Multiply $2^{10-(3+2)}$ by all numbers of two factors $< 2^5$.

$2^{10} = 2^{10-(3+3)} \cdot 2^{3+3}$

Multiply $2^{10-(3+3)}$ by all numbers of three factors $< 2^6$.

$2^{10} = 2^{10-(3+4)} \cdot 2^{3+4}$

Multiply $2^{10-(3+4)}$ by all numbers of four factors $< 2^7$.

$2^{10} = 2^{10-(3+5)} \cdot 2^{3+5}$

Multiply $2^{10-(3+5)}$ by all numbers of five factors $< 2^8$.

$2^{10} = 2^{10-(3+6)} \cdot 2^{3+6}$

Multiply $2^{10-(3+6)}$ by all numbers of six factors less than 2^9. Since we do not consider multiples of two, there are none, for $3^6 > 2^{6+3}$.

Then this last division adds no new composites to those already counted, and the number of composites of 10 - 3 factors less than 2^{10} is constant.

III. Composites Less Than $\lfloor n$.

A study was next made of the number intervals between factorial numbers. The method used was similar to that used in the previous study. However, instead of using factors of the form $(2+a_n)$ and determining the possible values of a_n, the possible prime factors, p, were found.

Here the number of factors possible in a composite less than the given number did not increase regularly, as before. Nor did the number of composites of any number of factors become constant.

Table II gives the results of the study of factorial numbers.

The following method was used in compiling table II.

$\lfloor 2 = 2$

There are no composites less than 2.

$\lfloor 3 = 6$

Composites of two factors:	No. of combinations
$p_1 = 2, p_2 = 2.$	1

$\lfloor 4 = 24$

Composites of two factors:	
$p_1 = 2$, $p_2 = 2$, 3, 5, 7, 11; $p_1 = 3$, $p_2 =$ 3, 5, 7.	8

Composites of three factors: No. of combinations

$p_1 = 2, p_2 = 2, p_3 = 2, 3, 5$

$p_1 = 2, p_2 = 3, p_3 = 3$ 4

Composite of four factors:

$p_1 = 2, p_2 = 2, p_3 = 2, p_4 = 2$ 1

Table II

Numbers less than:	$\lfloor 2$	$\lfloor 3$	$\lfloor 4$	$\lfloor 5$	$\lfloor 6$
Primes	1	4	10	31	129
Composites of 2 factors	0	1	8	39	218
" " " 3 " "	0	0	4	28	178
" " " 4 " "	0	0	1	15	103
" " " 5 " "	0	0	0	6	54
" " " 6 " "	0	0	0	2	22
" " " 7 " "	0	0	0	0	10
" " " 8 " "	0	0	0	0	4
" " " 9 " "	0	0	0	0	1

IV. Numbers of the form $6n \pm 1$ Between Powers of Five

If numbers having two and three as factors are eliminated, two thirds of the numbers are eliminated. Therefore a study was made of all composites between consecutive powers of five except those divisible by two and three. This included all numbers of the form $6n \pm 1$ in the interval studied.

The composites of the form $6n \pm 1$ were found by the method formerly used. The number of numbers of the form $6n \pm 1$ was found by finding the range of values n might take on. Then, since all primes > 3 are of the form $6n \pm 1$, the number of primes between any two numbers was found by subtracting the number of composites of the form $6n \pm 1$ from all the numbers of this form in the given interval.

In this case, the number of primes between two consecutive powers was studied rather than less than the given power. This necessitated finding a lower as well as an upper limit for the prime.

Table III gives the results of this study.

Method used in compiling table III.

As an example, take the interval 5^3 to 5^4.

Numbers of two factors of the form $6n \pm 1, < 5^4$ and $> 5^3$.

$p_1 = 5$, $p_2 = 29 - 113$

29 - 113 is to mean all primes from 29 to 113, including both numbers. No. of combinations

$p_1 = 7$, $p_2 = 19\text{-}89$; $p_1 = 11$, $p_2 = 13\text{-}53$;

$p_1 = 13$, $p_2 = 13\text{-}47$; $p_1 = 17$, $p_2 = 17\text{-}31$; 69

$p_1 = 19$, $p_2 = 19\text{-}31$; $p_1 = 23$, $p_2 = 23$.

Numbers of three factors of the form $6n \pm 1, < 5^4$ and $> 5^3$.

$p_1 = 5$, $p_2 = 5$, $p_3 = 7 - 23$;

$p_1 = 5$, $p_2 = 7$, $p_3 = 7 - 17$;

$p_1 = 5$, $p_2 = 11$, $p_3 = 11$; 13

$p_1 = 7$, $p_2 = 7$, $p_3 = 7 - 11$;

$21.6 + 1 = 127$ $22.6 - 1 = 131$

$103.6 + 1 = 619$ $104.6 - 1 = 623$

Consequently, there are 83 numbers of the form $6n + 1$ and 83 of the form $6n - 1 > 5^3$ and $< 5^4$.

Numbers of the form $6n + 1 > 5^3$ & $< 5^4 = 166$

Composites of the form $6n \pm 1 > 5^3$ & $< 5^4 - 82$

Primes of the form $6n \pm 1 > 5^3$ & $< 5^4$ - 84

Table III

Numbers of the form $6n \pm 1$ between

	$5 \& 5^2$	$5^2 \& 5^3$	$5^3 \& 5^4$	$5^4 \& 5^5$	$5^5 \& 5^6$
Primes	6	21	84	331	1376
Composites of 2 factors	0	11	69	376	1873
" " " 3 " "	0	0	15	111	766
" " " 4 " "	0	0	0	14	137
" " " 5 " "	0	0	0	0	14

Examination of the table shows that, as in the case of the powersof two, the number of composites of a given number of factors seems to be becoming constant.

A theorem analogous to the one on the powers of two is:-

Theorem II

The number of composites of the form $6n \pm 1$ of $n - n'$ factors between 5^{n-1} and 5^n becomes constant when $5^n \geqslant 5^k$ where k is the first number such that $7^k > 5^{n'+k}$.

Proof:

The number of composites of $n - n'$ factors less than a given number 5^n and greater than 5^{n-1} is found by taking $5^n = 5^{n-(n'+c)} \cdot 5^{n'+c}$ for all values of c from 1 to $n-n'$. If $5^{n-(n'+c)}$ is multiplied by all numbers of c factors less than $5^{n'+c}$ and greater than $5^{n'+c-1}$, it is evident that we have composites of $n - n'$ factors less than 5^n and greater than 5^{n-1}. However, in

counting the numbers of c factors less than $5^{n'+c}$ & greater than $5^{n'+c-1}$ we omit all those which contain 5 as a factor, except when c is 1, for these will have been counted previously with higher powers of five. Since we omit the composites with five as a factor, 7^c is the smallest number of c factors. If $7^c > 5^{n'+c}$ there are no numbers of c factors less than $5^{n'+c}$. Let k be the first value of c such that $7^c > 5^{n'+c}$. We then have $5^n = 5^{n-(n'+k)} \cdot 5^{n'+k}$. To get composites of n-n' factors, we multiply $5^{n-(n'+k)}$ by all numbers of k factors less than $5^{n'+k}$ and greater than $5^{n'+k-1}$. But there are no such numbers. Also, if $7^k > 5^{n'+k}$, then $7^{k+1} > 5^{n'+k+1}$, $7^{k+2} > 5^{n'+k+2}$, etc. That is, when $c \geq k$, there are no more composites of n-n' factors less than 5^n. Evidently, k does not depend on n, but on n'. Therefore, if n is large enough to allow these k divisions of 5^n, i. e., if $n \geq k$, the number of composites of n-n' factors is constant.

V. Factors of Fermat Numbers

Fermat suggested $2^{2^n}+1$ as a formula for prime numbers. However, only the first four have been found to be prime and twelve have been proved composite. The following is a table of the known results on Fermat numbers.[1]

Case		Factors of p	Discoverer	Year
1-5	0-4	All prime	Fermat	1640
6	5	$2^7.5+1=641$ $2^7.52347+1=6700417$	L. Euler	1729
7	6	Unknown but composite	Lucas	1878
		$2^8.9.7.17+1=274177$	Landry	1880
		$2^8.5.52562829149+1$	Landry & LeLasseam	1880
8	7	Unknown but composite	A. E. Western, J. C. Morehead	1905
9	8	Unknown but composite	A. E. Western, J. C. Morehead	1909
10	9	$2^{16}.37+1$	A. E. Western	1903
11	11	$2^{13}.3.13+1$ $2^{13}.7.17+1$	A. Cunningham	1809
12	12	$2^{14}.7+1$	E. Lucas & P. Pervúsin	1877
		$2^{16}.397+1$	A. E. Western	1903
		$2^{16}.7.139+1$		
13	18	$2^{20}.13+1$	A. E. Western	1903
14	23	$2^{25}.5+1$	P. Pervúsin	1878

1. Archibald, Amer. Math. Monthly, 21, (1914) pages 249

Case		Factors of p	Discoverer	Year
15	36	$2^{39}.5+1$	Seelhoff	1886
16	38	$2^{41}.3+1$	J. Cullen, A. Cunningham, A. E. & F. J. Western	1905
17	73	Unknown but composite	J. C. Morehead	1906
		$2^{75}.5+1$	J. C. Morehead	1906[2]

In this study, an attempt was made to determine factors of Fermat numbers by determining what numbers of the form $2^n.c$ p+1 could be factors of numbers of the form $2^{n'}$ +1, and which of these numbers were Fermat numbers. The residues of 2^n modulus 2^{n_1}. p + 1 might be computed by the following method. It was seen that the method was somewhat shortened if the last n residues before -1 were determined and the steps were made by 2^n rather than by two. The example gives this method in detail. Here the n, which is arbitrary, was chosen as 12. The residues to 2^{24} were determined simply by multiplying by 2. After 2^{24}, each number was multiplied by 2^{12} and each residue by the residue of 2^{12}. The residue of 2^{396} modulus 1793 was recognized as one of the twelve residues preceding -1, modulus 1793.

---

2. J. C. Morehead, Bulletin of the Am. Math. Soc. (1906) Vol. 12, pages 449-50.

$2^8 \cdot 7 + 1 = 1793$

$2^{11} \equiv 255 \mod 1793$

$2^{12} \equiv 510$

$2^{13} \equiv 1020$

$2^{14} \equiv 2040 \equiv 247$

$2^{15} \equiv 494$

$2^{16} \equiv 988$

$2^{17} \equiv 1976 \equiv 183$

$2^{18} \equiv 366$

$2^{19} \equiv 732$

$2^{20} \equiv 1464$

$2^{21} \equiv 2928 \equiv 1135$

$2^{22} \equiv 2270 \equiv 477$

$2^{23} \equiv 954$

$2^{24} \equiv 1908 \equiv 115$

$2^{36} \equiv 1274$

$2^{48} \equiv 674$

$2^{60} \equiv 1277$

$2^{72} \equiv 411$

$2^{84} \equiv 1622$

$2^{156} \equiv 1439 \mod 1793$

$2^{168} \equiv 553$

$2^{180} \equiv 529$

$2^{192} \equiv 840$

$2^{204} \equiv 1666$

$2^{216} \equiv 1571$

$2^{228} \equiv 1532$

$2^{240} \equiv 1365$

$2^{252} \equiv 466$

$2^{264} \equiv 984$

$2^{276} \equiv 1593$

$2^{288} \equiv 201$

$2^{300} \equiv 309$

$2^{312} \equiv 1599$

$2^{324} \equiv 1468$

$2^{336} \equiv 999$

$2^{348} \equiv 278$

$2^{360} \equiv 133$

$2^{372} \equiv 1489$

$2^{96} \equiv 647$

$2^{108} \equiv 58$

$2^{120} \equiv 892$

$2^{132} \equiv 1291$

$2^{144} \equiv 579$

$2^{384} \equiv 951$

$2^{396} \equiv 900$

$2^{397} \equiv 1800 \equiv 7$

$2^{398} \equiv 14$

$2^{399} \equiv 28$

$2^{400} \equiv 56 \bmod 1792$

$2^{401} \equiv 112$

$2^{402} \equiv 224$

$2^{403} \equiv 448$

$2^{404} \equiv 896$

$2^{405} \equiv 1792 \equiv -1 \bmod. 1793$

$2^{405} \equiv -1 \bmod. 1793$

$2^{405.2n} \equiv 1 \bmod 1793$

$2^{405(2n+1)} \equiv -1 \bmod 1793$

By a theorem due to Fermat, we know that $a^{\phi(m)} \equiv 1 \bmod m$ if a is prime to m. Then $a^{\frac{\phi(m)}{k}} \equiv -1 \bmod m$ if any power of a is congruent to -1 modulus m. $\phi(m)$ has the value,

$$\phi(m) = |m| \left(1 - \frac{1}{|p_1|}\right) \text{---------} \left(1 - \frac{1}{|p_r|}\right)$$

On account of the above, the work of the preceding example may be abbreviated as follows. If $a^{\frac{\phi(m)}{k}} \equiv -1 \bmod m$, k must evidently be a multiple of 2 for -1 must be multiplied by itself an even number of times to give a residue +1. It is then necessary only to find the even divisors of $\phi(m)$ and find the residue for these powers of two.

$\phi(1793) = \phi(11.163) = 10.162 = 1620$

$\frac{1620}{2} = 810$, $\frac{1620}{4} = 405$, $\frac{1620}{6} = 270$, $\frac{1620}{12} = 135$.

$2^{12} \equiv 510 \bmod 1793$

$2^{24} \equiv 115$

$2^{48} \equiv 674$

$2^{96} \equiv 647$

$\underline{2^{24} \equiv 115}$

$2^{120} \equiv 892$

$\underline{2^{15} \equiv 494}$

$2^{135} \equiv 1363$

$\underline{2^{270} \equiv 221}$

$2^{405} \equiv -1 \bmod 1793$

This method was used in compiling tables IV, V, and VI. However, Cunningham's Binary Canon[1] was used to determine the residues modulus $2^n.p\pm1$ when this modulus was prime and less than 1000.

1.Allan Cunningham, Binary Canon, London, 1900.

Table IV.

$2^n.3+1$	General exponent $\equiv -1$	Exponent in terms of ϕ function.
$2^1.3+1$	No power of 2 $\equiv -1$ mod 7	
$2^2.3+1$	$2^{6(2n+1)} \equiv -1$ mod 15	$\frac{\phi(15)}{2}(2n+1)$
$2^3.3+1$	$2^{10(2n+1)} \equiv -1$ mod 25	$\frac{\phi(25)}{2}(2n+1)$
$2^4.3+1$	No power of 2 $\equiv -1$ mod 49	
$2^5.3+1$	$2^{24(2n+1)} \equiv -1$ mod 97	$\frac{\phi(97)}{4}(2n+1)$
$2^6.3+1$	$2^{48(2n+1)} \equiv -1$ mod 193	$\frac{\phi(193)}{4}(2n+1)$
$2^7.3+1$	No power of 2 $\equiv -1$ mod 385	
$2^8.3+1$	$2^{192(2n+1)} \equiv -1$ mod 769	$\frac{\phi(769)}{4}(2n+1)$
$2^9.3+1$	$2^{182(2n+1)} \equiv -1$ mod 1537	$\frac{\phi(1537)}{8}(2n+1)$
$2^{10}.3+1$	No power of 2 $\equiv -1$ mod 3073	
$2^{11}.3+1$	$2^{614(2n+1)} \equiv -1$ mod 6145	$\frac{\phi(6145)}{8}(2n+1)$

Table V

$2^n.5+1$	General exponent $\equiv -1$	Exponent in terms of ϕ function
$2^1.5+1$	$2^{5(2n+1)} \equiv -1 \bmod 11$	$\frac{\phi(11)}{2}(2n+1)$
$2^2.5+1$	No power of $2 \equiv -1 \bmod 21$	
$2^3.5+1$	$2^{10(2n+1)} \equiv -1 \bmod 41$	$\frac{\phi(41)}{4}(2n+1)$
$2^4.5+1$	$2^{27(2n+1)} \equiv -1 \bmod 81$	$\frac{\phi(81)}{2}(2n+1)$
$2^5.5+1$	No power of $2 \equiv -1 \bmod 161$	
$2^6.5+1$	$2^{55(2n+1)} \equiv -1 \bmod 321$	$\frac{\phi(321)}{4}(2n+1)$
$2^7.5+1$	$2^{32(2n+1)} \equiv -1 \bmod 641$	$\frac{\phi(641)}{4.5}(2n+1)$
$2^8.5+1$	No power of $2 \equiv -1 \bmod 1281$	
$2^9.5+1$	$2^{294(2n+1)} \equiv -1 \bmod 2561$	$\frac{\phi(2561)}{8}(2n+1)$
$2^{10}.5+1$	No power of $2 \equiv -1 \bmod 5121$	
$2^{11}.5+1$	No power of $2 \equiv -1 \bmod 10241$	
$2^{12}.5+1$	$2^{3413(2n+1)} \equiv -1 \bmod 20481$	$\frac{\phi(2048)}{4}(2n+1)$

Table VI

$2^n.7+1$	General exponent $\equiv -1$	Exponent in terms of ϕ function
$2^1.7+1$	No power of 2 $\equiv -1$ mod 15	
$2^2.7+1$	$2^{14(2n+1)} \equiv -1$ mod 29	$\frac{\phi(29)}{2}(2n+1)$
$2^3.7+1$	$2^{9(2n+1)} \equiv -1$ mod 57	$\frac{\phi(57)}{4}(2n+1)$
$2^4.7+1$	$2^{14(2n+1)} \equiv -1$ mod 113	$\frac{\phi(113)}{8}(2n+1)$
$2^5.7+1$	No power of 2 $\equiv -1$ mod 225	
$2^6.7+1$	$2^{112(2n+1)} \equiv -1$ mod 449	$\frac{\phi(449)}{4}(2n+1)$
$2^7.7+1$	No power of 2 $\equiv -1$ mod 897	
$2^8.7+1$	$2^{405(2n+1)} \equiv -1$ mod 1793	$\frac{\phi(1793)}{4}(2n+1)$
$2^9.7+1$	No power of 2 $\equiv -1$ mod 3585	
$2^{10}.7+1$	$2^{1749(2n+1)} \equiv -1$ mod 7169	$\frac{\phi(7169)}{4}(2n+1)$
$2^{11}.7+1$	$2^{2349(2n+1)} \equiv -1$ mod 14337	$\frac{\phi(14337)}{4}(2n+1)$
$2^{12}.7+1$	$2^{3510(2n+1)} \equiv -1$ mod 28673	$\frac{\phi(28673)}{8}(2n+1)$
$2^{13}.7+1$	No power of 2 $\equiv -1$ mod 57345	
$2^{14}.7+1$	$2^{4096(2n+1)} \equiv -1$ mod 114689	$\frac{\phi(114689)}{4.7}(2n+1)$

This study of Fermat numbers yielded the following results:

Theorem I:

The numbers 13, 25, 49, 97, 193, 385, 769, 1537, 3073, 6145 of the form $2^n.3+1$, 11, 21, 41, 81, 161, 321, 1281, 2561, 5121, 10241, 20481, of the form $2^n.5+1$, 15, 29, 57, 113, 225, 449, 897, 1793, 3585, 7169, 14337, 28673, 57345, of the form $2^n.7+1$ cannot be factors of Fermat numbers.

Proof:

The multiples of 13 are of the form $2^{6(2n+1)}+1$. If 13 can be a factor of a number of the form $2^{2^n}+1$, $2^{6(2n+1)}+1$ must be of the form $2^{2^n}+1$; i. e.

$$12n+6 = 2^n$$

$$\text{or} \quad 3(2n+1) = 2^{n-1}$$

Obviously this cannot be true.

The method of proof was the same for each of the other numbers listed except those such that no number n could be found which satisfied the relation $2^n \equiv -1$ with the given number as modulus. An example of such a number is 15 which is $2^4.7+1$.

$2 \equiv 2 \bmod 15$

$2^2 \equiv 4 \bmod 15$

$2^3 \equiv 8 \bmod 15$

$2^4 \equiv 16 \equiv 1 \bmod 15$

$2^5 \equiv 2 \bmod 15$

All powers of two, then, are congruent to 1, 2, 4, or 8 mod 15. There is then no number n such that $2^n \equiv -1 \bmod 15$.

This is always the case when the modulus is of the form 2^n-1 for then it is not necessary to have the residue -1 to get the residue 1. If $2^{\frac{n}{2}}$ is squared, we have the residue 1.

Theorem II:

The numbers 641, i. e., $2^7 \cdot 5+1$, and 114689, i. e., $2^{14} \cdot 7+1$ are Factors of Fermat numbers.

Proof:

Multiples of 641 are of the form $2^{32(2n_1+1)}+1$. If these multiples are to be Fermat numbers, they must be of the form $2^{2^n}+1$, i. e.

$$32(2n_1+1)=2^n$$

$$\text{or } 2^5(2n_1+1)=2^n$$

This is true if $n_1=0$.

$\therefore$ 641 is a factor of $2^{2^5}+1$.

A similar proof holds for 114689 whose multiples are of the form $2^{4096(2n_1+1)}+1 = 2^{2^{12}(2n_1+1)}+1$.